UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/779,414	02/13/2004	Sanjay Kaniyar	13768.490	7773

22913 7590 11/10/2008

Workman Nydegger
1000 Eagle Gate Tower
60 East South Temple
Salt Lake City, UT 84111

EXAMINER	
DOAN, TRANG T	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
11/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/779,414	KANIYAR ET AL.	
	Examiner	Art Unit	
	TRANG DOAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is response to the amendment filed on 08/01/2008.

2. Claims 1, 3-4, 6-7, 9-11, 12-13, 15, 17-18, 20-21, 22-23, 25, 27-30, 32-33 and 35-36 have been amended.

3. Claim 2 has been canceled.

4. Claims 1 and 3-37 are pending for consideration.

Response to Arguments

5. Applicant's arguments with respect to claims 1, 3-11 and 22-28 have been considered but are moot in view of the new ground(s) of rejection.

6. Regarding claims 12-21 and 29-37, Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1, 18, 22 and 33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Regarding claim 1, 18, 22 and 33, Applicant recites the limitation "a second hash function that is more computationally intensive and more cryptographically secure than the first hash function" is not clear to Examiner. What does it mean to be more secure and more computationally intensive?

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 3-11 and 22-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldberg et al. (US 20040013112) (hereinafter Goldberg) in view of Wilson et al. (US 7159119) (hereinafter Wilson), and further in view of Hunt et al. (US 20030005306) (hereinafter Hunt).

Regarding claim 1, Roberts discloses in a local server that receives data from one or more remote entities over a data transport protocol, a method of applying a cryptographically secure hash to packets from unverified remote entities for preventing denial of service attacks on lookup tables used to store state information for one or more remote entities, while maintaining the performance of the local server for packets from verified remote entities, the method comprising the acts of:

(A) receiving a packet of data from a remote entity that includes connection identifier information (Goldberg: paragraphs 0014 and 0055: hashing a portion of the received packet);

(B) hashing at least a portion of the connection identifier information using a first hash function identifying an entry in a first table of verified remote entities, the entry containing state information for all packets comprising the first hash; and (Goldberg: paragraphs 0061-0062, 0066-0067 and 0071);

(C) determining if state information for the remote entity exists at the entry in the first table of verified remote entities (Goldberg: paragraph 0059: session recognition is performed whereby the session database is searched for a socket matching that of the received packet);

(a) wherein if it is determined the state information for the remote entity does exist in the first table of verified remote entities, performing standard data transport protocol on the packet of data (Goldberg: paragraph 0062: if a session having a socket matching that of the received packet is found, the session data is read from the session database and the session data then processed); and

(b) providing program modules for performing the following when it is determined that the state information for the remote entity does not exist in the table of verified remote entities (Goldberg: paragraph 0059: if a match was not found, a static rules check is performed using a static filter and paragraphs 0060-0061):

(ii) determining if state information for the remote entity exists at the second entry in the second table of unverified remote entities (Goldberg: paragraph 0014);

(1) wherein if it is determined that the state information for the remote entity exists in the second table of unverified remote entities, comparing secret information provided within the packet of data with information previously supplied to the remote entity for determining if the remote entity can be verified such that state information can be moved to the table of verified remote entities (Goldberg: paragraphs 0114); and

(2) wherein if it is determined that the state information for the remote entity does not exist in the second table of unverified remote entities (Goldberg: paragraphs 0059, 0072-0073 and 0082-0084); checking whether the local server is a listener that may accept the packet of data from the remote entity for determining if the state information for the remote entity should be created in the second table of unverified remote entities (Goldberg: paragraphs 0060-0061 and 0071-0072).

Goldberg does not explicitly disclose two lookup tables (i.e., the table of verified remote entities and the table of unverified remote entities). However, Wilson discloses two lookup tables (Wilson: See Abstract section and column 4 lines 50-54). Therefore, it would have been obvious to one having ordinary skill in the art at the time the

invention was made to modify Goldberg by specifically providing the features, as taught by Wilson, because it is well known in the art at the time of the invention for the purpose of retrieving information from a secured data store that securely pre-processes provided access information and provides efficient retrieval of address information (Wilson: column 2 lines 20-24).

Goldberg in view of Wilson does not explicitly disclose (i) hashing at least a portion of the connection identifier information using a second hash function that is more computationally intensive and more cryptographically secure than the first hash function, resulting in a second hash which is less predictable than the first hash generated by the first hash function, the second hash identifying another entry in a second table of unverified remote entities, the second entry containing state information for all packets comprising the second hash. However, Hunt discloses (i) hashing at least a portion of the connection identifier information using a second hash function that is more computationally intensive and more cryptographically secure than the first hash function, resulting in a second hash which is less predictable than the first hash generated by the first hash function, the second hash identifying another entry in a second table of unverified remote entities, the second entry containing state information for all packets comprising the second hash (Hunt: paragraphs 0015 and 0030). Therefore, it would have been obvious to a person skilled art at the time the invention was made to have included in Goldberg in view of Wilson the feature of Hunt as discussed above because by using a cryptographic hash function a relatively short but highly unique identifier. Additionally, such a hash would provide a short, 20 bytes long

identifier for a file of any size thereby allowing for very quick comparisons (Hunt: paragraph 0027).

Regarding claim 3, Goldberg as modified discloses wherein the standard data transport protocol is transmission control protocol (Goldberg: paragraphs 0002, 0009 and 0048).

Regarding claims 4 and 23, Goldberg as modified discloses wherein if the state information for the remote entity exists in the second table of unverified remote entities, but the remote entity cannot be verified, the method further comprises the act of: checking if the packet includes a synchronization message for determining how to respond to the unverified remote entity (Goldberg: See figure 9).

Regarding claims 5 and 24, Goldberg as modified discloses wherein if the packet of data includes a synchronization message, the local server responds by either sending a synchronization-acknowledgement packet or by deleting the packet (Goldberg: See figure 9).

Regarding claims 6 and 25, Goldberg as modified discloses wherein if the packet of data does not include a synchronization message, the local server responds by one or more of the following deleting the packet, retransmitting the original message to the remote entity or removing the state information from the second table of unverified remote entities (Goldberg: paragraphs 0015 and 0016).

Regarding claim 7, Goldberg as modified discloses wherein the first hash function is also a cryptographically secured hash function (Goldberg: paragraphs 0014 and 0058).

Regarding claim 8, Goldberg as modified discloses wherein the first and second hash functions are one of hardware based or software based (Goldberg: paragraph 0014).

Regarding claims 9 and 27, Goldberg as modified discloses wherein if state information for the remote entity does not exist in either the first table of verified remote entities or the second table of unverified remote entities, and wherein the server is a listener that may accept the package of data from the remote entity, the method further comprising the acts of: creating state information for the remote entity within the table of unverified remote entities; and sending a synchronization-acknowledgement packet that includes an initial sequence number to the remote entity (Goldberg: See figure 9 and Wilson: See Abstract section and column 4 lines 50-54). The same motivation was utilized in claim 1 applied equally well to claim 9.

Regarding claims 10 and 28, Goldberg as modified discloses wherein if state information for the remote entity does not exist in either the first table of verified entities or the second table of unverified entities, and the server is not a listener that may accept the package of data from the remote entity, the method further comprises the act of: sending a reset command to the remote entity for indicating that the packet was not verifiable and needs to be resent (Goldberg: See figure 9 and paragraphs 0061-0062 and 0124 and Wilson: See Abstract section and column 4 lines 50-54). The same motivation was utilized in claim 1 applied equally well to claim 10.

Regarding claim 11, Goldberg as modified discloses wherein the remote entity becomes verified by sharing a secret sent to the remote entity by the local server (Goldberg: paragraphs 0056-0057 and 0066-0067).

Regarding claim 22, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Regarding claim 26, Goldberg as modified discloses wherein the first hash function is also a cryptographically secured hash function, and wherein the first and second hash functions are one of either hardware based or software based (Goldberg: paragraph 0014).

12. Claims 12-17, 19-21, 29-32 and 34-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldberg et al. (US 20040013112) (hereinafter Goldberg) in view of Wilson et al. (US 7159119) (hereinafter Wilson).

Goldberg discloses a method of applying a cryptographically secure hash to packets from unverified remote entities for preventing denial of service attacks on lookup tables used to store state information for one or more remote entities, while maintaining the performance of the local server for packets from verified remote entities, the method comprising: an act of receiving a packet of data from a remote entity that includes connection identifier information (Goldberg: see figure 3 and paragraph 0059); a step for determining if state information exists for the remote entity in a first table of verified remote entities (Goldberg: paragraph 0059); if the state information for the remote entity does not exist in the first table of verified remote entities, a step for determining if state information exists for the remote entity in a second table of

unverified remote entities (Goldberg: paragraph 0085: a hole table); if the state information exists in the second table of unverified remote entities, a step for determining if the remote entity can be verified such that state information can be moved to the first table of verified remote entities (Goldberg: paragraph 0086); if state information does not exist in the second table of unverified remote entities (Goldberg: paragraphs 0090-0092 and 0097); a step for determining if state information for the remote entity should be created in the second table of unverified remote entities (Goldberg: paragraphs 0090-0092 and 0097).

Goldberg does not explicitly disclose two lookup tables (i.e., the table of verified remote entities and the table of unverified remote entities). However, Wilson discloses two lookup tables (Wilson: See Abstract section and column 4 lines 50-54). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Goldberg by specifically providing the features, as taught by Wilson, because it is well known in the art at the time of the invention for the purpose of retrieving information from a secured data store that securely pre-processes provided access information and provides efficient retrieval of address information (Wilson: column 2 lines 20-24).

Regarding claim 13, Goldberg as modified discloses wherein if the state information for the remote entity does exist in the table of verified remote entities, standard data transport protocol processing is performed (Goldberg: paragraphs 0002, 0009 and 0048).

Regarding claim 14, Goldberg as modified discloses wherein the standard data transport protocol is transmission control protocol (Goldberg: paragraphs 0002, 0009 and 0048).

Regarding claims 15 and 30, Goldberg as modified discloses wherein if the state information for the remote entity exists in the second table of unverified remote entities, but the remote entity cannot be verified, the method further comprises the act of: checking if the packet includes a synchronization message for determining how to respond to the unverified remote entity (Goldberg: See figure 9).

Regarding claims 16 and 31, Goldberg as modified discloses wherein if the packet of data includes a synchronization message, the local server responds by either sending a synchronization-acknowledgement packet or by deleting the packet (Goldberg: See figure 9).

Regarding claims 17 and 32, Goldberg as modified discloses wherein if the packet of data does not include a synchronization message, the local server responds by one or more of the following deleting the packet, retransmitting the original message to the remote entity or removing the state information from the second table of unverified remote entities (Goldberg: paragraphs 0015 and 0016).

Regarding claim 19, Goldberg as modified discloses wherein the first hash function is also a cryptographically secured hash function, and wherein the first and second hash functions are one of either hardware based or software based (Goldberg: paragraph 0014).

Regarding claims 20 and 35, Goldberg as modified discloses creating state information for the remote entity within the second table of unverified remote entities; and sending a synchronization-acknowledgement packet that includes an initial sequence number to the remote entity (Goldberg: paragraphs 0060, 0109 and 0111-0115).

Regarding claims 21 and 36, Goldberg as modified discloses sending a reset command to the remote entity for indicating that the packet was not verifiable and needs to be resent (Goldberg: See figure 9 and paragraphs 0061-0062 and 0124 and Wilson: See Abstract section and column 4 lines 50-54). The same motivation was utilized in claim 12 applied equally well to claim 21.

Regarding claim 29, this claim has limitations that is similar to those of claim 12, thus it is rejected with the same rationale applied against claim 12 above.

Regarding claim 34, this claim has limitations that is similar to those of claim 19, thus it is rejected with the same rationale applied against claim 19 above.

Regarding claim 37, Goldberg as modified discloses wherein the remote entity becomes verified by sharing a secret sent to the remote entity by the local server (Goldberg: paragraphs 0056-0057 and 0066-0067).

13. Claims 18 and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldberg et al. (US 20040013112) (hereinafter Goldberg) in view of Wilson et al. (US 7159119) (hereinafter Wilson), and further in view of Hunt et al. (US 20030005306) (hereinafter Hunt).

Regarding claim 18, Goldberg discloses wherein the step for determining if state information exists for the remote entity in the first table of verified remote entities includes the act of hashing at least a portion of the connection identifier information using a first hash function, and wherein the step for determining if state information exists for the remote entity in a second table of unverified remote entities includes the act of hashing at least a portion of the connection identifier information using a second hash function (Goldberg: paragraphs 0009 and 0014: a first hash calculation…a second hash calculation). Golden does not explicitly disclose the second hash function that is more computationally intensive and more cryptographically secure than the first hash function, resulting in a second hash which is less predictable than a first hash generated by the first hash function.

However, Hunt discloses the second hash function that is more computationally intensive and more cryptographically secure than the first hash function, resulting in a second hash which is less predictable than a first hash generated by the first hash function (Hunt: paragraphs 0015 and 0030). Therefore, it would have been obvious to a person skilled art at the time the invention was made to have included in Goldberg in view of Wilson the feature of Hunt as discussed above because by using a cryptographic hash function a relatively short but highly unique identifier. Additionally, such a hash would provide a short, 20 bytes long identifier for a file of any size thereby allowing for very quick comparisons (Hunt: paragraph 0027).

Regarding claim 33, this claim has limitations that is similar to those of claim 18, thus it is rejected with the same rationale applied against claim 18 above.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

15. Examiner's Note: Examiner has cited particular columns and line numbers in the references applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

16. In the case of amending the claimed invention, Applicant is respectfully requested to indicate the portion(s) of the specification which dictate(s) the structure relied on for proper interpretation and also to verify and ascertain the metes and bounds of the claimed invention.

17. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431

/Syed Zia/
Primary Examiner, Art Unit 2431